16/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2008 Elsevier Eng. Info. Inc. All rts. reserv.

11896551 E.I. No: EIP074010847516
Title: Learning attack strategies through mining and correlation of security alarms
Author: Li, Wang; Zhi-tang, Li; Jie, Lei
Corporate Source: Computer Science Department Huazhong University of Science and Technology, Hubei, Wuhan, China
Conference Title: 10th IFIP/IEEE International Symposium on Integrated Network Management 2007, IM '07
Conference Location: Munich, Germany Conference Date: 20070521-20070525
E.I. Conference No.: 70289
Source: 10th IFIP/IEEE International Symposium on Integrated Network Management 2007, IM '07 10th IFIP/IEEE International Symposium on Integrated Network Management 2007, IM '07 2007.
Publication Year: 2007
ISBN: 9781424407996
DOI: 10.1109/INM.2007.374834
Article Number: 4258586
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical); X; (Experimental)
Journal Announcement: 0710W2
Abstract: Huge volume of security data from **different** security **devices** can overwhelm security managers and keep them from performing effective analysis and initiating timely response. Therefore, it is important to develop an advanced alert correlation system that can reduce alert redundancy, intelligently correlate security **alerts** and detect attack strategies. In this paper, we proposed a new method of mining multi-stage attack behaviors pattern in order to recognize attacker's high-level strategies and predict upcoming attack intentions. We apply a reformative Apriori algorithm to mine frequent attack sequence patterns from **history alert** data. We use correlativity between two contextual elements in the attack sequence to correlate attack behaviors and identify potential attack intentions. The idea is easy to implement and it can be used to detect novel multi-stage attack strategies compared with other techniques. Experiments show that our approach can effectively learn high level attack strategies and can accordingly predict next possible attack behavior. copy 2007 IEEE. 15 Refs.
Descriptors: *Computer crime; Algorithms; Artificial intelligence; Correlation methods; Data mining; Learning systems; **Network security**
Identifiers: Attack sequence patterns; Security devices; Apriori algorithms; Multi-stage attack behaviors
Classification Codes:
723.2 (Data Processing); 723.4 (Artificial Intelligence); 922.2 (Mathematical Statistics)
723 (Computer Software, Data Handling & Applications); 922 (Statistical Methods)
72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

16/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2008 Elsevier Eng. Info. Inc. All rts. reserv.

11841945 E.I. No: EIP073510787948
Title: Data fusion support for intrusion detection and prevention
Author: Beheshti, Mohsen; Wasniowski, Richard A.
Corporate Source: Computer Science Department California State University Dominguez Hills
Conference Title: 4th International Conference on Information Technology-New Generations, ITNG 2007
Conference Location: Las Vegas, NV, United States Conference Date: 20070402-20070404
Sponsor: Premier Hall for Science and Engineering (PHASE)
E.I. Conference No.: 70126
Source: Proceedings - International Conference on Information Technology-New Generations, ITNG 2007 Proceedings - International Conference on Information Technology-New Generations, ITNG 2007 2007. (IEEE cat n P2776)

Publication Year: 2007
ISBN: 9780769527765
DOI: 10.1109/ITNG.2007.62
Article Number: 4151825
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 0709WI
Abstract: The main problem with current intrusion detection and prevention systems is high rate of false alarms triggered off by **attackers**. Effective protecting the **network** against **attacks** remains problem in both research and the computer network managing professionals. Improved monitoring of malicious attacks will require integration of multiple monitoring systems. In our project we are analyzing potential benefits of distributed **multi sensor** systems for intrusion detection. Our main purpose for this work is to examine how to integrate **multiple** intrusion detection **sensors** in the order to minimize the number of incorrect-alarms. The first problem is how to integrate data from **multiple sensors**, and the second how to identify most important data provided by **multiple sensors**. We are currently developing series of analytical models to use potential benefits of **multiple sensors** for reducing false alarms. The purpose of this presentation is to discuss implementation of prototype multisensor based intrusion detection system. We are especially interested in analyzing traffic that has an abnormal or malicious character and should prompt a closer look. A specific feature of the model is that the systems use **multiple sensors** to process log files. This reduces the overhead in a distributed intrusion detection system. The Snort left bracket 1 right bracket based **multiple sensors** system monitors two networks. Our configuration allows generating Snort events with identical timestamps to ensure that we can successfully merge data from **multiple** snort **sensors** with identical timestamps. On both networks one web server is an Intel-based PC running Microsoft Windows 2003, the **second** web **server** is Centos based Linux system. Each Snort sensor is an Intel-based PC running CENTOS4.3/4.4 with Snort 2.3/2.6 and mySQL 4.3.10. Snort sensors are configured with identical rule sets to run in Intrusion Detection System mode, and to **log** to the MySQL database and **alerts log** files. In addition to monitoring online traffic we simulate attacks and the attacker system is an Intelbased PC running Fedora Core (FC4) laptop computer. The system is implemented using Open Software whenever possible such as Snort, Honeypot, mySQL etc. We have collected a large amount of data such as **alert logs** and multiple mySQL databases and improved snort rules design and we are currently finalizing processing those sets of data. This project is described in details on web site left bracket 4 right bracket. On the whole, our information fusion based intrusion detection and prevention model is in fact a prototype and needs to evolve into more mature and efficient model. Future work emphasizes a revisit of database design to allow more efficient data fusion from **multiple sensors**. 4 Refs.
Descriptors: *Intrusion detection; Computer networks; Laptop computers; Problem solving; Sensor data fusion; Telecommunication traffic
Identifiers: Database design; Open Software; Online traffic; Snort sensors
Classification Codes:
723.4 (Artificial Intelligence); 723.2 (Data Processing); 722.4 (Digital Computers & Systems)
723 (Computer Software, Data Handling & Applications); 716 (Electronic Equipment, Radar, Radio & Television); 722 (Computer Hardware)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATION ENGINEERING)

16/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

11238139 E.I. No: EIP06391012900
Title: Filtering false alarms: An approach based on episode mining
Author: Bodon, Ferenc; Hornak, Zoltan
Corporate Source: Budapest University of Technology and Economics, H-1117 Budapest, Hungary
Source: Periodica Polytechnica, Electrical Engineering v 49 n 1-2 2005. p 3-23
Publication Year: 2005

CODEN: PPYTA7 ISSN: 0324-6000
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 0609W5
Abstract: The security of computer networks is a prime concern today. **Various devices** and methods have been developed to offer different kinds of protection (firewalls, **IDS**'s, antiviruses, etc.). By centrally storing and processing the signals of these devices, it is possible to detect more cheats and attacks than simply by analysing the **logs** independently. The most difficult and still unsolved problem in centralized systems is that vast numbers of false **alarms**. If a harmless pattern, which caused by a safe operation is identified as an **alarm**, then it is a nuisance and requires human invention to be handled properly. In this paper we show how we can use data mining to discover the patterns that frequently causes false alarms. Due to the new requirements (events with many attributes, invertible parametric predicates) none of the previously published algorithms can be applied to our problem directly. We present the algorithm ABAMSEP, which discovers frequent alert-ended episodes. We prove that the algorithm is correct in the sense that it finds all episodes that meet the requirements of the specification. 16 Refs.
Descriptors: *Data mining; Computer networks; Alarm systems; **Viruses**; Signal processing; Problem solving; Algorithms
Identifiers: Remote supervision system; Antiviruses; Human invention
Classification Codes:
723.2 (Data Processing); 914.1 (Accidents & Accident Prevention); 461.9 (Biology); 716.1 (Information & Communication Theory); 723.4 (Artificial Intelligence)
723 (Computer Software, Data Handling & Applications); 914 (Safety Engineering); 461 (Bioengineering); 716 (Electronic Equipment, Radar, Radio & Television)
72 (COMPUTERS & DATA PROCESSING); 91 (ENGINEERING MANAGEMENT); 46 (BIOENGINEERING); 71 (ELECTRONICS & COMMUNICATION ENGINEERING)

16/5/4 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2008 Elsevier Eng. Info. Inc. All rts. reserv.

09110055 E.I. No: EIP02337050808
Title: Multivariate statistical analysis of audit trails for host-based intrusion detection
Author: Ye, Nong; Emran, Syed Masum; Chen, Qiang; Vilbert, Sean
Corporate Source: Arizona State University, Tempe, AZ 85287-5906, United States
Source: IEEE Transactions on Computers v 51 n 7 July 2002. p 810-820
Publication Year: 2002
CODEN: ITCOB4 ISSN: 0018-9340
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical); X; (Experimental)
Journal Announcement: 0208W3
Abstract: Intrusion detection complements prevention mechanisms, such as firewalls, cryptography, and authentication, to capture intrusions into an information system while they are acting on the information system. Our study investigates a multivariate quality control technique to detect intrusions by building a long-term profile of normal activities in information systems (norm profile) and using the norm profile to detect anomalies. The multivariate quality control technique is based on Hotelling's T**2 test that detects both counterrelationship **anomalies** and mean-shift **anomalies**. The performance of the Hotelling's T**2 test is **examined** on **two** sets of **computer audit data**: a small data set and a large multiday data set. Both data sets contain sessions of normal and intrusive activities. For the small data set, the Hotelling's T**2 test signals all the intrusion sessions and produces no false **alarms** for the normal sessions. For the large data set, the Hotelling's T**2 test signals 92 percent of the intrusion sessions while producing no false alarms for the normal sessions. The performance of the Hotelling's T**2 test is also compared with the performance of a more scalable multivariate technique - a chi-squared distance test. 28 Refs.
Descriptors: *Security of data; Computer system firewalls; Cryptography; Information science; Data mining; Statistical tests; Statistical process

control; Mathematical models; Matrix algebra; Computational complexity
Identifiers: Audit trails; Intrusion detection; Multivariate statistical analysis; Chi-square test; Information system
Classification Codes:
723.2 (Data Processing); 903.1 (Information Sources & Analysis); 922.2 (Mathematical Statistics); 731.1 (Control Systems); 921.6 (Numerical Methods); 921.1 (Algebra)
723 (Computer Software, Data Handling & Applications); 903 (Information Science); 922 (Statistical Methods); 731 (Automatic Control Principles & Applications); 921 (Applied Mathematics)
72 (COMPUTERS & DATA PROCESSING); 90 (ENGINEERING, GENERAL); 92 (ENGINEERING MATHEMATICS); 73 (CONTROL ENGINEERING)

16/5/5 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online
(c) 2008 ProQuest Info&Learning. All rts. reserv.

02202533 ORDER NO: AADAA-I1440768
ARF: An automated real-time fuzzy logic threat evaluation system
Author: Gray, Jeremy D.
Degree: M.Eng.
Year: 2006
Corporate Source/Institution: University of Louisville (0110)
Adviser: James Graham
Source: VOLUME 45/03 of MASTERS ABSTRACTS.
PAGE 1530. 147 PAGES
Descriptors: COMPUTER SCIENCE
Descriptor Codes: 0984

Intrusion Detection has emerged as a powerful component of **network security** systems. A wide range of hardware and software components exist to meet most basic security needs on all platforms. These systems **log** system usage that could be considered as a breach of security in many networks. However, signature based intrusion detection systems have one catastrophic downfall, in that the number of **alerts** being logged can quickly outgrow the amount of resources necessary to investigate this anomalous behavior. This thesis explores the use of a fuzzy logic based analysis engine that gives an overall threat level of an intrusion detection sensor, prioritizing alerts that are the most threatening. This application gives security personnel a launching point to determine where security holes exist and a snapshot of the threats that exist in a system.
The fuzzy logic system is based on a set of membership functions that define certain metrics from an alert dataset and a set of rules that determine a threat level based on the defined metrics. This application functions as a proof of concept prototype for an administrative tool that can analyze **multiple sensors** across multiple networks and give a reasonable output of the threat level across a series of intrusion detection sensors on a network. Initial testing indicates promising performance results for testing the threat level of a remote sensor using this methodology.

16/5/6 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2008 Institution of Electrical Engineers. All rts. reserv.

10832758
Title: Hop-count monitoring: detecting sinkhole attacks in wireless sensor networks
Author(s): Dallas, D.; Leckie, C.; Ramamohanarao, K.
Author Affiliation: Melbourne Univ., Melbourne, Australia
Conference Title: 2007 15th IEEE International Conference on Networks p.176-81
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 2007 Country of Publication: USA
ISBN: 978-1-4244-1229-7 Material Identity Number: YXA8-1900-209
Conference Title: 2007 15th IEEE International Conference on Networks
Conference Date: 19-21 Nov. 2007 Conference Location: Adelaide, SA, Australia
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P); Theoretical (T)

Abstract: We investigate the problem of defending wireless sensor networks against attacks that disrupt dynamic routing protocols. We propose a novel intrusion detection system that detects the presence of a sinkhole attack, or any attack that misleads traffic by understating the cost of an attack route. Our study shows that protocols designed to select the shortest path between **two nodes** will, through time, select a series of paths whose length exhibits a **log** -normal distribution. By **deriving** tolerance limits from the lognormal distribution of path lengths under normal conditions, we develop an **anomaly** detection scheme that detects sinkhole attacks in a computationally efficient manner. We show that our scheme can detect attacks with 96% accuracy and no false **alarms** using a single detection system in a simulated network. (12 Refs)

Subfile: B

Descriptors: log normal distribution; routing protocols; telecommunication network management; telecommunication security; wireless sensor networks

Identifiers: hop-count monitoring; sinkhole attack detection; wireless sensor networks; dynamic routing protocols; intrusion detection system; log-normal distribution; anomaly detection scheme

Class Codes: B6250 (Radio links and equipment); B6210C (Network management); B6150M (Protocols); B6150P (Communication network design, planning and routing); B0240Z (Other topics in statistics)

16/5/7 (Item 2 from file: 2)

09598961 INSPEC Abstract Number: C2005-11-6150N-289

Title: Mining logs files for computing system management

Author(s): Wei Peng; Tao Li; Sheng Ma

Author Affiliation: Sch. of Comput. Sci., Florida Int. Univ., Miami, FL, USA

Conference Title: Proceedings. Second International Conference on Autonomic Computing p.309-10

Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA

Publication Date: 2005 Country of Publication: USA xiii+396 pp.

ISBN: 0 7695 2276 9 Material Identity Number: XX-2005-01003

U.S. Copyright Clearance Center Code: 0 7695 2276 9/2005/$20.00

Conference Title: Proceedings. Second International Conference on Autonomic Computing

Conference Sponsor: IEEE Comput. Soc.; Nat. Sci. Found

Conference Date: 13-16 June 2005 Conference Location: Seattle, WA, USA

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: With advancement in science and technology, computing systems become increasingly more difficult to monitor, manage and maintain. Traditional approaches to system management have been largely based on domain experts through a knowledge acquisition process to translate domain knowledge into operating rules and policies. This has been experienced as a cumbersome, labor intensive, and error prone process. There is thus a pressing need for automatic and efficient approaches to monitor and manage complex computing systems. A popular approach to system management is based on analyzing system log files. However, several new aspects of the system log data have been less emphasized in existing analysis methods and posed several challenges. The aspects include disparate formats and relatively short text messages in data reporting, asynchronous data collection, and temporal characteristics in data representation. First, a typical computing system contains **different devices** with different software components, possibly from different providers. These various components have multiple ways to report events, conditions, errors and **alerts** . The heterogeneity and **inconsistency** of **log** formats make it difficult to automate problem **determination** . To perform automated analysis, we need to categorize the text messages with disparate formats into common situations. Second, text messages in the log files are relatively short with a large vocabulary size. Third, each text message usually contains a timestamp. The temporal characteristics provide additional context information of the messages and can be used to facilitate data analysis. In this paper, we apply text mining to automatically categorize the messages into a set of common categories, and propose two approaches of incorporating temporal information to improve the categorization performance. (4 Refs)

Subfile: C
Descriptors: Bayes methods; data mining; data structures; message passing ; object-oriented programming
Identifiers: log file mining; computing system management; system monitoring; system maintenance; knowledge acquisition; domain knowledge; operating rules; operating policies; system log file analysis; data reporting; asynchronous data collection; temporal characteristics; data representation; software components; log format heterogeneity; log format inconsistency; text message categorization; context information; data analysis; text mining
Class Codes: C6150N (Distributed systems software); C6120 (File organisation); C6170K (Knowledge engineering techniques); C6110J (Object-oriented programming); C1140Z (Other topics in statistics)

16/5/8 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

08550582 INSPEC Abstract Number: C2003-04-0310-011
Title: The importance of event correlation for effective security management
Author(s): Caldwell, M.
Journal: Information Systems Control Journal vol.6 p.36-8
Publisher: Inf. Syst. Audit. & Control Assoc,
Publication Date: 2002 Country of Publication: USA
CODEN: ISYJFS ISSN: 1526-7407
SICI: 1526-7407(2002)6L.36:IECE;1-J
Material Identity Number: H454-2002-006
U.S. Copyright Clearance Center Code: 1526-7407/02/$2.50+0.25
Language: English Document Type: Journal Paper (JP)
Treatment: General, Review (G)
Abstract: Security teams try to detect attacks and internal misuse by wading through and making sense of an overwhelming amount of raw event data generated from firewalls, intrusion detection systems, vulnerability reports, routers, computer systems and other devices. This process does not provide the coherent view of their networks necessary to successfully manage threats. A solution for this problem is an emerging security category called security event management (SEM). SEM systems automatically aggregate and correlate security event log data across **multiple** types of security **devices** allowing security analysts to focus on critical tasks that require human intelligence, such as investigating the source of attacks and responding to them. There are a wide variety of SEM solutions, but at the core of all of these solutions is the ability to correlate **alerts** across a heterogeneous security environment. Correlation of **event data** is critical to uncover security breaches because security incidents are made up of a series of events that occur at various touch points throughout a network. Unlike network management, which typically is exception-based or a one-to-one process, security management is far more complex. An **attack** typically touches a **network** at multiple points and leaves marks or breadcrumbs at each. By finding and following that breadcrumb trail, a security analyst can detect and hopefully prevent the attack.
Subfile: C
Descriptors: business data processing; DP management; information systems ; security of data
Identifiers: event correlation; enterprise information security; security event management; security event log data; heterogeneous security environment; alerts
Class Codes: C0310 (EDP management); C6130S (Data security); C7100 (Business and administration)

16/5/9 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

08220190 INSPEC Abstract Number: C2002-04-6130S-076
Title: Computer security: hacking tendencies, criteria and solutions
Author(s): Botha, M.; von Solms, R.

Author Affiliation: Dept. of Inf. Technol., Port Elizabeth Univ., South Africa
Conference Title: Hardware, Software and Peopleware. South African Institute of Computer Scientist and Information Technologists Annual Conference p.81-7
Editor(s): Renaud, K.; Kotze, P.; Barnard, A.
Publisher: Unisa Press, Pretoria, South Africa
Publication Date: 2001 Country of Publication: South Africa xix+226 pp.
ISBN: 1 86888 195 4 Material Identity Number: XX-2001-02851
Conference Title: Proceedings of SAICSIT 2001. South African Institute of Computer Science and Information Technology Annual Conference
Conference Date: 25-28 Sept. 2001 Conference Location: Pretoria, South Africa
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Computer crime and **more** particularly **computer hacking** has become increasingly active in today's business environment. Proof of this statement is a survey completed by the Computer Security Institute and the FBI which revealed that corporations, banks and governments all face a growing threat from computer crime (Berst, 1999). Different methods can be used to control access to computer networks such as firewalls, but none is **hacker** -proof. New ways and means must therefore be defined which will minimise or eliminate computer crime. These ways should involve the utilisation of audit **logs** and user profiles in a proactive sense. Typical proactive actions that can be defined include: online monitoring, template analysis, generation of reports and generation of **alert** signals. The objective of the paper is to define and describe a proactive model which will identify a **hacking** attempt before it has been performed, on any computer system with more effective and easy to use graphical interfaces. This model should also provide useful tools for the security officer. It will inform the officer of different levels of **hacking** attempts according to statistical predefined norms. (14 Refs)
Subfile: C
Descriptors: computer crime
Identifiers: computer security; **hacking** tendencies; computer crime; computer **hacking**; business environment; Computer Security Institute; FBI; corporations; banks; governments; firewalls; audit logs; user profiles; proactive actions; online monitoring; template analysing; reports generation; alert signals generation; graphical interfaces; security officer; statistical predefined norms
Class Codes: C6130S (Data security); C0230 (Economic, social and political aspects of computing); C0310D (Computer installation management)

16/5/10 (Item 5 from file: 2)

08077245 INSPEC Abstract Number: B2001-12-6210C-033, C2001-12-6130S-041
Title: Security management: making sense of events
Author(s): King, C.M.
Journal: Business Communications Review vol.31, no.9 p.32, 35-8
Publisher: BCR Enterprises,
Publication Date: Sept. 2001 Country of Publication: USA
CODEN: BCCRBD ISSN: 0162-3885
SICI: 0162-3885(200109)31:9L.32:SMMS;1-0
Material Identity Number: F939-2001-010
U.S. Copyright Clearance Center Code: 0162-3885/2001/$0.00+.50
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: Security event management promises clarity amid the alarms. The typical large enterprise routinely is inundated with security-related **alerts** from heterogeneous security devices (intrusion detection systems, firewalls, VPN gateways and platforms). **Network security** managers are awakened at all hours by various events that seem to demand their immediate attention. These managers find themselves attempting manually to inspect or decipher reports of security anomalies from amid the reams of **logs** generated by their organization's **array** of security **devices** -an impossible task. To make sense of all this information, security managers need an operational view of the security health of the enterprise. This

article looks at strategies to **alert** properly, categorize and react to security events as they occur. Security event management is a combination of the **security** and **network** management disciplines. It requires not only the proper infrastructure, but the correct processes. An enterprise trying to implement SEM today faces an impressive integration challenge. (0 Refs)
Subfile: B C
Descriptors: business communication; computer network management; security of data; telecommunication security
Identifiers: security event management; security-related alerts; heterogeneous security devices; intrusion detection system; firewalls; VPN gateways; platforms; **network security** managers
Class Codes: B6210C (Network management); B6210L (Computer communications); C6130S (Data security)

16/5/13 (Item 1 from file: 95)

02004593 20051003710
Mining logs files for computing system management
Peng, Wei; Li, Tao; Ma, Sheng
School of Comput. Sci., Florida Internat. Univ., Miami, US
Second Internat. Conf. on Autonomic Computing, Proc., Seattle, US, 13-16 June 20052005
Document type: Conference paper Language: English
Record type: Abstract
ISBN: 0-7695-2276-9

ABSTRACT:
With advancement in science and technology, computing systems become increasingly more difficult to monitor, manage and maintain. Traditional approaches to system management have been largely based on domain experts through a knowledge acquisition process to translate domain knowledge into operating rules and policies. This has been experienced as a cumbersome, labor intensive, and error prone process. There is thus a pressing need for automatic and efficient approaches to monitor and manage complex computing systems. A popular approach to system management is based on analyzing system log files. However, several new aspects of the system log data have been less emphasized in existing analysis methods and posed several challenges. The aspects include disparate formats and relatively short text messages in data reporting, asynchronous data collection, and temporal characteristics in data representation. First, a typical computing system contains **different devices** with different software components, possibly from different providers. These various components have multiple ways to report events, conditions, errors and **alerts** . The heterogeneity and **inconsistency** of **log** formats make it difficult to automate problem **determination** . To perform automated analysis, we need to categorize the text messages with disparate formats into common situations. Second, text messages in the log files are relatively short with a large vocabulary size. Third, each text message usually contains a timestamp. The temporal characteristics provide additional context information of the messages and can be used to facilitate data analysis. In this paper, we apply text mining to automatically categorize the messages into a set of common categories, and propose two approaches of incorporating temporal information to improve the categorization performance.

DESCRIPTORS: BAYES METHOD; DATA FORMAT; OBJECT ORIENTED PROGRAMMING; SYSTEM CONTROL; KNOWLEDGE ACQUISITION; INFORMATION PRESENTATION; DATA ANALYSIS
IDENTIFIERS: BEREICHSKENNTNIS; BETRIEBLICHE POLITIK; ZEITLICHE KENNZEICHNUNG; SOFTWARE KOMPONENTE; KONTEXTINFORMATION; TEXTSCHUERFEN; Bayes-Verfahren; Datengewinnung

12/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2008 The Gale Group. All rts. reserv.

02095368 SUPPLIER NUMBER: 19709010 (USE FORMAT 7 OR 9 FOR FULL TEXT)
KSM makes sense of NT logs; Intrusion Detection's burglar alarm provides near-real-time alerting. (Intrusion Detection's Kane Security Monitor) (Software Review)(Evaluation)
Phillips, Ken
PC Week, v14, n36, p110(2)
August 25, 1997
DOCUMENT TYPE: Evaluation ISSN: 0740-1604 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1244 LINE COUNT: 00102

... be especially useful to enterprise network managers struggling to consolidate and interpret auditing data from **multiple** NT **servers**.
+ Automatically combines security event-**log** data from **multiple servers**; compiles **analysis** into attractive graphs and reports; **alerts** administrators to present **threats**; easy to install and use; automatically sets NT auditing options.
- Does not scan E-mail...

...block connections with prohibited hosts; does not detect network attacks on most services; has limited **alerting** capabilities.
Scoring methodology: www.pcweek.com/reviews/meth.htm
Intrusion Detection Inc., New York (800...

...the data into coherent patterns, expose dangers using three-dimensional graphs and printed reports, and **alert** administrators to security threats in near-real time.
KSM does not, however, **alert** administrators to outside network service attacks (such as PING floods or denial-of-service attacks...

12/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2008 The Gale Group. All rts. reserv.

02039791 SUPPLIER NUMBER: 19148556 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Cybercops. (Internet Security Systems)(Company Profile)
Moukheiber, Zina
Forbes, v159, n5, p170(2)
March 10, 1997
DOCUMENT TYPE: Company Profile ISSN: 0015-6914 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1047 LINE COUNT: 00079

... a piece of software that captures passwords on the network.
The ISS program sends a **warning** flag. Scanning can take anywhere from five minutes to a month, depending on the number...

...camera inside a network of up to 50 computers. The administrator can thus keep a **log** on all transactions and **look** for **suspicious** activity.
Novell was the first to license Klaus' scanner, for $20,000--a number Klaus...

...asked to see a demo of Klaus' software. A few minutes into the demo an **alarm** went off. The scanner had broken into the classified Jet Propulsion Laboratory and pulled a...
...price list. Current prices: $10 to $80 per computer for the scanner, depending on how **many computers** are on your network. The monitor costs $5,000.
The 75 employees of ISS work...

12/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2008 The Gale Group. All rts. reserv.

01806286 SUPPLIER NUMBER: 17082862 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Power management systems.
Sliter, Tom
STACKS, v2, n10, p41(7)
Oct, 1994
ISSN: 1070-8596 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4958 LINE COUNT: 00402

... server or workstation.
PowerAlert Plus software monitors power data from a SMART Series UPS. Custom **alarms** can be set on the console, as well as remote testing for the UPS systems...

...pulling on-line and historical information from servers and workstations on the UPS systems. All **detected** power **irregularities** are consolidated in a single Master Network Power **Log** by PowerAlert Plus. See Figure 4 for a view of the PowerMen Plus console.
The software pools **alarms** from all Tripp Lite LAN UPSs, and from most of the competition's models. The...

...you to be at a workstation to review power events.
PowerAlert Plus lets you customize **alarm** set points for load percentage, battery charge level, input voltage, and tIPS internal temperature. Conditions can be monitored on4ine, but when **alarms** are tripped, entries are created in the Master Log. PowerAlert Plus also lets you schedule...and save the profile for later recall. This tool is userid for the management of **many** SNMP **devices** on a network, not just UPS systems. The profiles are launched from the MIB browser...

12/3,K/4 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2008 The Gale Group. All rts. reserv.

02999870 Supplier Number: 78723532 (USE FORMAT 007 FOR FULLTEXT)
GuardedNet Joins OPSEC Alliance for Internet Security Interoperability.
Business Wire, p0108
Sept 28, 2001
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 614

... of customers, SOCs and Managed Security Service Providers (MSSP), and users."
Large, global networks have **many different** security **devices** and systems from many vendors, with differing abilities to **log** security events or block attacks. Typically, these networks include Intrusion **Detection** Systems (IDS), firewalls, servers, and routers. NeuSecure, a new class of **threat** management software for information security operations, aggregates **threat** information from **multi**-vendor, **multi**-**device** networks to improve enterprise security, delivering real-time **threat** analysis and response capability to security **analysts**. NeuSecure solves the issue of "**Log** data overload" by consolidating **log** data from your many security products, correlating the data, and then identifying the "real" **threat** - hastening critical decisions and response.
NeuSecure functionality provides security management and reporting, correlating events and **alerts** generated by OPSEC-compliant security solutions to provide event monitoring and analysis.
About GuardedNet(TM..

12/3,K/5 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2008 The Gale Group. All rts. reserv.

02854795 Supplier Number: 73017102 (USE FORMAT 007 FOR FULLTEXT)
Cisco Announces Next Generation Graphical Interface for Security and Virtual Private Network -- VPN -- Products.
Business Wire, p0348
April 10, 2001
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 711

... tools deliver and complement Cisco's overall security management strategy consisting of single-device management, **multi - device** management, such as CiscoWorks2000, and end-to-end policy-based management, such as Cisco Secure...

...At a glance, administrators can view graphical reports summarizing network activity, resource utilization and event **logs**, allowing performance and trend **analysis**. PDM's logging and **notification** features also allow security staff to detect and interrupt **suspicious** activity.
The embedded design of these device managers enables Cisco customers to manage PIX firewalls...

12/3,K/6 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2008 The Gale Group. All rts. reserv.

02128122 Supplier Number: 55246446 (USE FORMAT 007 FOR FULLTEXT)
Trend Micro Delivers Updated Microsoft Exchange Email Virus Protection with New Content Filtering and Spam Blocking Functionality.
Business Wire, p0058
July 26, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1386

... be accessed remotely from any NT server on the network.
Emergency File Blocking -- For virus **alert** situations, administrators can use this feature to block incoming files by file name, type, etc., (the recent ExploreZip wormfile attachment, for instance) while still permitting other non-**threatening** email to pass through. Blocked files can either be deleted or quarantined. An extensive **log** of all blocked files is automatically generated for later **analysis** and inspection.
Active Update Technology -- ScanMail now automatically updates and installs new scan engine, pattern file and program files simultaneously to **multiple** Exchange **servers** via a single button click without the need to reboot enabling a quick response to...scan engine, pattern file and product version is running on a particular server and automatically **notifies** the administrator if any of the ScanMail servers is inactive or has stopped functioning.
ScanMail for Exchange can be centrally deployed to **multiple** Exchange **servers**, which can all be configured updated, and managed from Trend Micro's web-based central...

12/3,K/7 (Item 4 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2008 The Gale Group. All rts. reserv.

02118345 Supplier Number: 55148583 (USE FORMAT 007 FOR FULLTEXT)
Network Associates Ships CyberCop Sting - Industry's First 'Decoy' Server Silently Traces and Tracks Hacker Activity.
PR Newswire, p0970
July 14, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 726

... IP network on a single server or workstation and can simulate a network containing several **different** types of network **devices**, including Windows NT servers, Unix servers and routers. Each virtual network device has a real...

...it becomes a problem."
CyberCop Sting provides a number of benefits for security administrators, including:
* **Detection** of **suspicious** activity inside network; **Log** files serve to
alert administrators to potential attackers prying into reserved areas.

* Ability to record **suspicious** activity without sacrificing any real
systems or protected information.
* Virtual decoy network can contain multiple...

12/3,K/8 (Item 5 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01211842 Supplier Number: 43635822 (USE FORMAT 007 FOR FULLTEXT)
ETHERPROBE NETWORK PROTOCOL ANALYZER ADDS NETWORK ANALYSIS FUNCTIONS
News Release, p1
Feb 8, 1993
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 480

... IBM
LAN Server, and TCP/IP protocols, it also enables a network manager to set **alarms** on nearly 50 conditions related to LAN stability based on traffic analysis, including excessive or unusually low densities of **various** request types, **server** announcements, logins, broadcasts,
and other phenomena. When **abnormal** conditions arise, EtherProbe's **alarms detect** them, **log** them to a file, issue optional popups on the
screen, and can even trigger capture...

12/3,K/9 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03323027 Supplier Number: 46831546 (USE FORMAT 7 FOR FULLTEXT)
AXENT TECHNOLOGIES: AXENT announces availability of real-time monitoring and intrusion detection for NT
M2 Presswire, pN/A
Oct 28, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 770

RDATE:281096
AXENT Technologies Inc. (NASDAQ:AXNT), Monday announced the availability of its OmniGuard/Intruder **Alert** (ITA) version 2.3 for Windows NT. This release of ITA gives users the ability...

...have enough people to review those logs. In addition, because these logs are produced by **multiple servers** running multiple operating systems, it is difficult to correlate audit events across different platforms. Even if **suspicious** activity is **discovered** in the audit **logs**, it is often too late to do anything about it," said Pete Privateer, AXENT's...

12/3,K/10 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

08124027 Supplier Number: 66886942 (USE FORMAT 7 FOR FULLTEXT)
Cybercrime: Get A Clue.(Industry Trend or Event)
DeVoney, Chris
Sm@rt Partner, v3, n35, p52
Oct 2, 2000
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1306

... from the academic and Unix worlds. These products do far more than just sound the **alarm**; they predict security problems, help assess the extent of damage, are instrumental in prosecuting cyberoffenders, and may undo some of the damage.

Simply put, an IDS is a combination early- **warning** system and post-event auditing tool. The system works by examining and reporting security incidents...

...by the firewall can signal an impending denial of service (DoS) attack.
Important Clues Like **many** other **computer** subjects, IDSes have certain features over which many competitive claims are made. Some areas are...
...some only offer one or the other. Real-time work lets the IDS sound the **alarm** to the staff. The downside is that real-time analysis requires substantial computing power and...

...security events that don't require a real-time response and by applying several statistical **analyses** on the **logs** **looking** for **anomalies**. If you have a choice, go for an IDS with both capabilities.
Sensor Placement Where...

12/3,K/11 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07027263 Supplier Number: 59459238 (USE FORMAT 7 FOR FULLTEXT)
Web attackers run roughshod; BY SANDRA GITTLEN, ELLEN MESSMER AND DENISE PAPPALARDO. (Industry Trend or Event)
Network World, p1
Feb 14, 2000
Language: English Record Type: Fulltext
Document Type: Tabloid; Trade
Word Count: 1255

(USE FORMAT 7 FOR FULLTEXT)

ABSTRACT:
TEXT:
...distributed type operate on the idea that the attacker, with client software, can remotely control **several** **servers** to launch the attacks through a "master" server. "To my knowledge, the attack came from..

...news site gets 2.5 million page views each day. CNN, which uses six ISPs, **noticed** problems with its routers at around 7 p.m last Tuesday. "The attack was broadly...
...working realized the attack was on, at about 7 a.m last Tuesday, they started **looking** for **suspicious** traffic patterns in the server **logs** and upstream routers. After SYN flooding was **determined** to be the cause, GTE Internetworking began filtering out illegitimate traffic at the router. Cooper...

12/3,K/12 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06264334 Supplier Number: 54352512 (USE FORMAT 7 FOR FULLTEXT)
In Focus: Intrusion Detection Security Mandate: Silence False Alarms. (Company Business and Marketing)
Yasin, Rutrell
InternetWeek, p1(1)
April 12, 1999
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 1024

... a machine was transmitting legitimate data, according to Kondilas.
To avoid being overwhelmed by false **alarms**, IT managers at Qwest are documenting each false positive. By recording exactly what is happening in the network at the time an **alarm** triggered, operators can determine if similar events in the future are false **alarms**, he said.
Since network- and host-based systems each have strengths and weaknesses, some vendors...

...determine if the cause is a hacker or a bad router, and they also can

look into the event log to see if there is suspicious activity, Hodges said.

Both Axent and ISS introduced hybrid systems last year. ISS RealSecure can pull information from multiple network sensors and systems agents to track activity across a range of devices and systems. But that...

12/3,K/13 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2008 The Gale Group. All rts. reserv.

05198275 Supplier Number: 47931330 (USE FORMAT 7 FOR FULLTEXT)
KSM Makes Sense of NT Logs; Intrusion Detection's burglar alarm provides near-real-time alerting
Phillips, Ken
PC Week, p110
August 25, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 1171

... be especially useful to enterprise network managers struggling to consolidate and interpret auditing data from multiple NT servers.

+ Automatically combines security event-log data from multiple servers; compiles analysis into attractive graphs and reports; alerts administrators to present threats; easy to install and use; automatically sets NT auditing options.

- Does not scan E-mail...

...block connections with prohibited hosts; does not detect network attacks on most services; has limited alerting capabilities.

Scoring methodology: www.pcweek.com/reviews/meth.html

Intrusion Detection Inc., New York (800...

...the data into coherent patterns, expose dangers using three-dimensional graphs and printed reports, and alert administrators to security threats in near-real time.

KSM does not, however, alert administrators to outside network service attacks (such as PING floods or denial-of-service attacks...

12/3,K/14 (Item 5 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2008 The Gale Group. All rts. reserv.

04892969 Supplier Number: 47196458 (USE FORMAT 7 FOR FULLTEXT)
Cybercops
Moukheiber, Zina
Forbes, p170
March 10, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; General Trade
Word Count: 993

... a piece of software that captures passwords on the network.

The ISS program sends a warning flag. Scanning can take anywhere from five minutes to a month, depending on the number...

...camera inside a network of up to 50 computers. The administrator can thus keep a log on all transactions and look for suspicious activity.

Novell was the first to license Klaus' scanner, for $20,000--a number Klaus...

...asked to see a demo of Klaus' software. A few minutes into the demo an alarm went off. The scanner had broken into the classified Jet Propulsion Laboratory and pulled a...
...price list. Current prices: $10 to $80 per computer for the scanner, depending on how many computers are on your network. The monitor costs $5,000.

The 75 employees of ISS work...

12/3,K/15 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2008 The Gale Group. All rts. reserv.

08759997 SUPPLIER NUMBER: 18310211 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Spies like us. (increasing internet security risks, corporate sabotage) (includes related articles on increasing security, a glossary and information resources) (Internet/Web/Online Service Information)
Young, Jeffrey
Forbes, v157, n11, p70(14)
June 3, 1996
ISSN: 0015-6914 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 8225 LINE COUNT: 00664

... complex blueprints for electronic devices that take years to perfect.
In September 1994, Cadence grew **suspicious** of engineer Mitsuru "Mitch" Igusa when he left the company and refused to sign a confidentiality agreement. **Checking** computer **logs**, the company's internal networking staff **discovered several** very large **computer** file transfers to Igusa's home machine, recorded days before his departure. Believing they were...

...to resolve software discrepancies between a Cadence product and a competing application from Avant!. He **noticed** a bug in Avant!'s software--a bug he had originally created in the Cadence...

12/3,K/16 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2008 The Gale Group. All rts. reserv.

03327230 SUPPLIER NUMBER: 06233837 (USE FORMAT 7 OR 9 FOR FULL TEXT)
When the headlines hit home. (catastrophic risk assessment)
Vollenweider, Dale
Best's Review - Life-Health Insurance Edition, v88, n8, p22(4)
Dec, 1987
ISSN: 0005-9706 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 2751 LINE COUNT: 00230

... catastrophic risk associated with their client groups that are partially self-funded. Such insurers should **inform** their clients of their potential catastrophic losses and help them to avoid, reduce or transfer this risk. While experience-refund pooling schemes provide some catastrophic risk-sharing, **many** group **clients** prefer the peace of mind that comes with guaranteed-premium catastrophe reinsurance protecting their own...

...member of a known concentration. When applications come in from other members of the same **risk** group--teammates on the same sports team, for example--a quick **check** of the **log**'s entries will **determine** whether the acceptance of this application will lead to a catastrophic **risk** overretention.
Although this method is not foolproof, it can help point to some large potential...

12/3,K/17 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2008 The Gale Group. All rts. reserv.

02035401 SUPPLIER NUMBER: 03252191 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Microcomputers in microbiology: a matter of special needs.
Harrell, Lizzie J.
Medical Laboratory Observer, v16, p57(5)
May, 1984
ISSN: 0580-7247 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 2200 LINE COUNT: 00174

... furnish some date processing capability. Over the long term, we would work with manufacturers on **more** thorough **computer** programs.

Since our mainframe hospital computer is basically an information system--transferring lab results to...

...QC was a system that would monitor media input and output and store performance testing **checks** and equipment maintenance **logs**. As to flagging **unusual** results, we **identified** three areas where a computer could save us time identifying **unusual** microbes, spotting **unusual** antibiotic susceptibility patterns, and **alerting** us to the circumstances of several specimens from the same site on a given patient...

12/3,K/18 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2008 ProQuest Info&Learning. All rts. reserv.

01986686 49752364
Web attackers run roughshod
Gittlen, Sandra; Messmer, Ellen; Pappalardo, Denise
Network World v17n7 PP: 1, 10 Feb 14, 2000
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 1502

...TEXT: distributed type operate on the idea that the attacker, with client software, can remotely control **several** **servers** to launch the attacks through a master" server

"To my knowledge, the attack came from..

...news site gets 2.5 million page views each day. CNN, which uses six ISPs, **noticed** problems with its routers at around 7 p.m last Tuesday"The attack was broadly...

...Internetworking realized the attack was on, at about 7 a.m last Tuesday, they started **looking** for **suspicious** traffic patterns in the server **logs** and upstream routers.
After SYN flooding was **determined** to be the cause, GTE Internetworking began filtering out illegitimate traffic at the router. Cooper...

12/3,K/19 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2008 ProQuest Info&Learning. All rts. reserv.

01220843 98-70238
Spies like us
Young, Jeffrey
Forbes ASAP Supplement PP: 70-92 Jun 3, 1996
ISSN: 0015-6914 JRNL CODE: FBR
WORD COUNT: 3189

...TEXT: complex blueprints for electronic devices that take years to perfect.

In September 1994, Cadence grew **suspicious** of engineer Mitsuru "Mitch" Igusa when he left the company and refused to sign a confidentiality agreement. **Checking** computer **logs**, the company's internal networking staff **discovered** **several** very large **computer** file transfers to Igusa's home machine, recorded days before his departure. Believing they were...

...to resolve software discrepancies between a Cadence product and a competing application from Avant!. He **noticed** a bug in Avant!'s software--a bug he had originally created in the Cadence...

12/3,K/20 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2008 ProQuest Info&Learning. All rts. reserv.

00643981 92-58921
Day Care: Insurers Are Taking Another Look
Diaz, Lisa

Rough Notes v135n10 PP: 16-17 Oct 1992
ISSN: 0035-8525 JRNL CODE: RNO
WORD COUNT: 1253

...TEXT: is still in some respects problematic, but feels it has shown some improvement. "I've **noticed** a change of attitude. In the past, the main concern of insurers has been about...

...but there are always qualifications that must be satisfied before a policy is sold. In **many** instances, prospective **clients** must complete applications describing all aspects of the operation and the facility must undergo an inspection. The company then **looks** at the credentials and past claims **history** of the operator, **evaluates** the grounds for potential hazards, and makes its final decision based on its findings.

There are some **risks** that insurers are just not willing to take, however. In-home facilities, which many parents...

12/3,K/21 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01189245 CMP ACCESSION NUMBER: INW19990412S0008
In Focus: Intrusion Detection - Security Mandate: Silence False Alarms
Rutrell Yasin
INTERNETWEEK, 1999, n 760, PG1
PUBLICATION DATE: 990412
JOURNAL CODE: INW LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: News & Analysis
WORD COUNT: 1030

... take intrusion detection to the next level, as more companies use the high-tech burglar **alarms** to identify attacks from outsiders as well as insiders.

IT managers looking for ways to reduce false-positive **alarms** cited the need for better event correlation.

Robert Kondilas, a security manager at carrier Qwest...

...SANS Institute, a training and consulting firm, said, "The huge load of not-very-important **alarms** has caused a complete shift in the way people do network-based ID." He added...
...that the beeper goes off so often that they can't possibly respond to every **alarm**.

The false-positive problem is generally confined to network-based intrusion detection systems that monitor...

...packet-flooding attacks, rather than the host-based systems that monitor PC server and firewall **logs** for **suspicious** activity.

For example, an intrusion **detection** systems may confuse port scans from a network management tool such as Hewlett-Packard's...

...a machine was transmitting legitimate data, according to Kondilas.

To avoid being overwhelmed by false **alarms**, IT managers at Qwest are documenting each false positive. By recording exactly what is happening in the network at the time an **alarm** triggered, operators can determine if similar events in the future are false **alarms**, he said.

Since network- and host-based systems each have strengths and weaknesses, some vendors...

...determine if the cause is a hacker or a bad router, and they also can **look** into the event **log** to see if there is **suspicious** activity, Hodges said.

Both Axent and ISS introduced hybrid systems last year. ISS

RealSecure can pull information from **multiple** network **sensors** and systems agents to track activity across a range of devices and systems. But that...

12/3,K/22 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2008 CMP Media, LLC. All rts. reserv.

01098269 CMP ACCESSION NUMBER: WIN19960801S0126
WinMag's Web Woes
David W. Methvin
WINDOWS MAGAZINE, 1996, n 708, PG176
PUBLICATION DATE: 960801
JOURNAL CODE: WIN LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Cover Story
WORD COUNT: 239

In running the security check on our own site, we discovered **several** of the Web **server** security holes discussed in this article. We did a mediocre job on the security checklist...

...samples and which were really necessary for operation. We didn't keep up with security **alerts**, and we didn't check for vendor updates. In addition, while testing the CGI scripting...

...a sensitive program file in the CGI directory. Finally, three **different** people were responsible for **different** aspects of **server** operation. When files were changed or created, it was easy to assume that it was...

...mapped out responsibilities, so it's clear who needs to take care of what. We **check** regularly for **unusual** occurrences in the server **logs** now... and we're a lot more paranoid.
Copyright (c) 1996 CMP Media Inc.

12/3,K/23 (Item 1 from file: 674)
DIALOG(R)File 674:Computer News Fulltext
(c) 2006 IDG Communications. All rts. reserv.

098970
QWEST CYBER SOLUTIONS BEEFS UP SECURITY
Byline: JENNIFER MEARS
Journal: Network World
Publication Date: January 28, 2002
Word Count: 545 Line Count: 54

Text:
... SERVER OPERATING SYSTEM AND APPLICATIONS, PROVIDING 24-7 MONITORING OF FILES, SYSTEM APPLICATIONS AND APPLICATION **LOGS** TO **DETECT UNUSUAL** ACTIVITY. CUSTOMERS RECEIVE REPORTS, **THREAT ANALYSIS** AND RECOMMENDATIONS TO STOP ATTACKS. * NETWORK INTRUSION DETECTION. THIS IS OFFERED IN TWO PACKAGES. THE...

... WHICH ARE PLACED WITHIN THE CIRCUIT TO TRANSPARENTLY MONITOR NETWORK TRAFFIC 24X7. EVENTS TRIGGER AN **ALERT** TO QCS, WHICH **NOTIFIES** THE CUSTOMER AND WORKS WITH THE CUSTOMER TO CORRECT THE PROBLEM. CUSTOMERS RECEIVE REPORTS, THREAT ANALYSIS AND RECOMMENDATIONS TO STOP ATTACKS. THE **SECOND** PACKAGE INCLUDES STANDARD **SENSORS** THAT TRANSPARENTLY MONITOR THE NETWORK 24X7. WHEN AN EVENT IS DETECTED, QCS IS **ALERTED** AND **NOTIFIES** THE CUSTOMER. * STRONG AUTHENTICATION. THIS ADDS A SECOND LEVEL OF AUTHENTICATION SECURITY BEYOND USERNAME AND...

12/3,K/24 (Item 2 from file: 674)
DIALOG(R)File 674:Computer News Fulltext
(c) 2006 IDG Communications. All rts. reserv.

081546
Web attackers run roughshod

BY SANDRA GITTLEN, ELLEN MESSMER AND DENISE PAPPALARDO
Journal: Network World Page Number: 1
Publication Date: February 14, 2000
Word Count: 1218 Line Count: 115

Text:
... distributed type operate on the idea that the attacker, with client software, can remotely control **several** **servers** to launch the attacks through a "master" server. "To my knowledge, the attack came from..

... news site gets 2.5 million page views each day. CNN, which uses six ISPs, **noticed** problems with its routers at around 7 p.m last Tuesday. "The attack was broadly...

... working realized the attack was on, at about 7 a.m last Tuesday, they started **looking** for **suspicious** traffic patterns in the server **logs** and upstream routers. After SYN flooding was **determined** to be the cause, GTE Internetworking began filtering out illegitimate traffic at the router. Cooper...

12/3,K/25 (Item 3 from file: 674)
DIALOG(R)File 674:Computer News Fulltext
(c) 2006 IDG Communications. All rts. reserv.

078886
Stealthy Trojan Horse attempts to gather data on Web sites
Byline: Sean M. Dugan
Journal: Network World
Publication Date: October 22, 1999
Word Count: 411 Line Count: 38

Text:
... file. Upon reboot, its.exe tries to retrieve another its.dat file from one of **several** Web **servers** on the Internet. The purpose of the its.dat file is not clear, as it...

... s investigation is still underway, and it is recommending that network administrators take note of **unusual** port activity on ports 8080 and 3128. It also recommends that administrators who **notice** **unusual** activity should **check** their servers' **logs** for **unusual** connections and their directories for **odd** or unfamiliar cgi scripts. The SANS Institute, in Bethesda, Md., is at www.sans.org.

12/3,K/26 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0854653 BW1014

CENTRAX: Year 2000 Wire/Centrax Announces Availability of eNTrax Security Suite for Windows NT

May 26, 1998

Byline: Business Editors/Computer Writers

...detection and response technologies in a single solution, allowing system administrators to single-handedly manage **multiple** **computers** across the enterprise from one central location. eNTrax minimizes the MIS resources needed to administer security over the enterprise by providing efficient **threat** detection and response solutions, effective audit policy creation and management, centralized event **log** **analysis** and **assessment**, deterrence and attack anticipation.
Paul E. Proctor, chief technical officer of Centrax states, "Insider misuse...

...controls and firewalls
can't address. eNTrax acts like a video surveillance system for computers, **notifying** security personnel of possible breaches in security and then identifying the perpetrators."

Combining expert security...

12/3,K/27 (Item 2 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0638277 BW1071

AXENT TECHNOLOGIES: AXENT Technologies Inc., announces availability of real-time monitoring and intrusion detection for Windows NT

October 28, 1996

Byline: Business Editors/Computers & Electronics Writers

...1996--AXENT(TM)
Technologies Inc. (NASDAQ:AXNT), Monday announced the availability
of its OmniGuard/Intruder **Alert** (ITA) version 2.3 for Windows NT.
This release of ITA gives users the ability...

...have enough people to review those logs. In addition,
because these logs are produced by **multiple servers** running multiple
operating systems, it is difficult to correlate audit events across
different platforms. Even if **suspicious** activity is **discovered** in
the audit **logs**, it is often too late to do anything about it," said
Pete Privateer, AXENT's...

12/3,K/28 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1281142 LATU037
Centrax Announces Availability of eNTrax Security Suite for Windows NT

DATE: May 26, 1998 06:00 EDT WORD COUNT: 900

... detection and response technologies in a single solution, allowing system administrators to single-handedly manage **multiple computers** across the enterprise from one central location. eNTrax minimizes the MIS resources needed to administer security over the enterprise by providing efficient **threat** detection and response solutions, effective audit policy creation and management, centralized event **log analysis** and **assessment**, deterrence and attack anticipation.

Paul E. Proctor, chief technical officer of Centrax states, "Insider misuse...

... controls and firewalls can't address. eNTrax acts like a video surveillance system for computers, **notifying** security personnel of possible breaches in security and then identifying the perpetrators."

Combining expert security...

12/3,K/29 (Item 1 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2008 Business Wire. All rts. reserv.

00496554 20010410100B6185 (USE FORMAT 7 FOR FULLTEXT)
Cisco Announces Next Generation Graphical Interface for Security and Virtual Private Network -- VPN -- Products-Easy to Use GUIs Deliver Powerful Management and Monitoring Tools
Business Wire
Tuesday, April 10, 2001 09:01 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 734

...tools deliver and complement Cisco's
overall security management strategy consisting of single-device

management,
multi-device management, such as CiscoWorks2000, and end-to-end policy-based
management, such as Cisco Secure...

...At a glance,
administrators can view graphical reports summarizing network activity,
resource utilization and event logs, allowing performance and trend analysis.
PDM's logging and notification features also allow security staff to detect
and interrupt suspicious activity.

The embedded design of these device managers enables Cisco customers to manage
PIX firewalls...